RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: IDY-F01

The Emperor's New Password Manager: Security Analysis of Password Managers

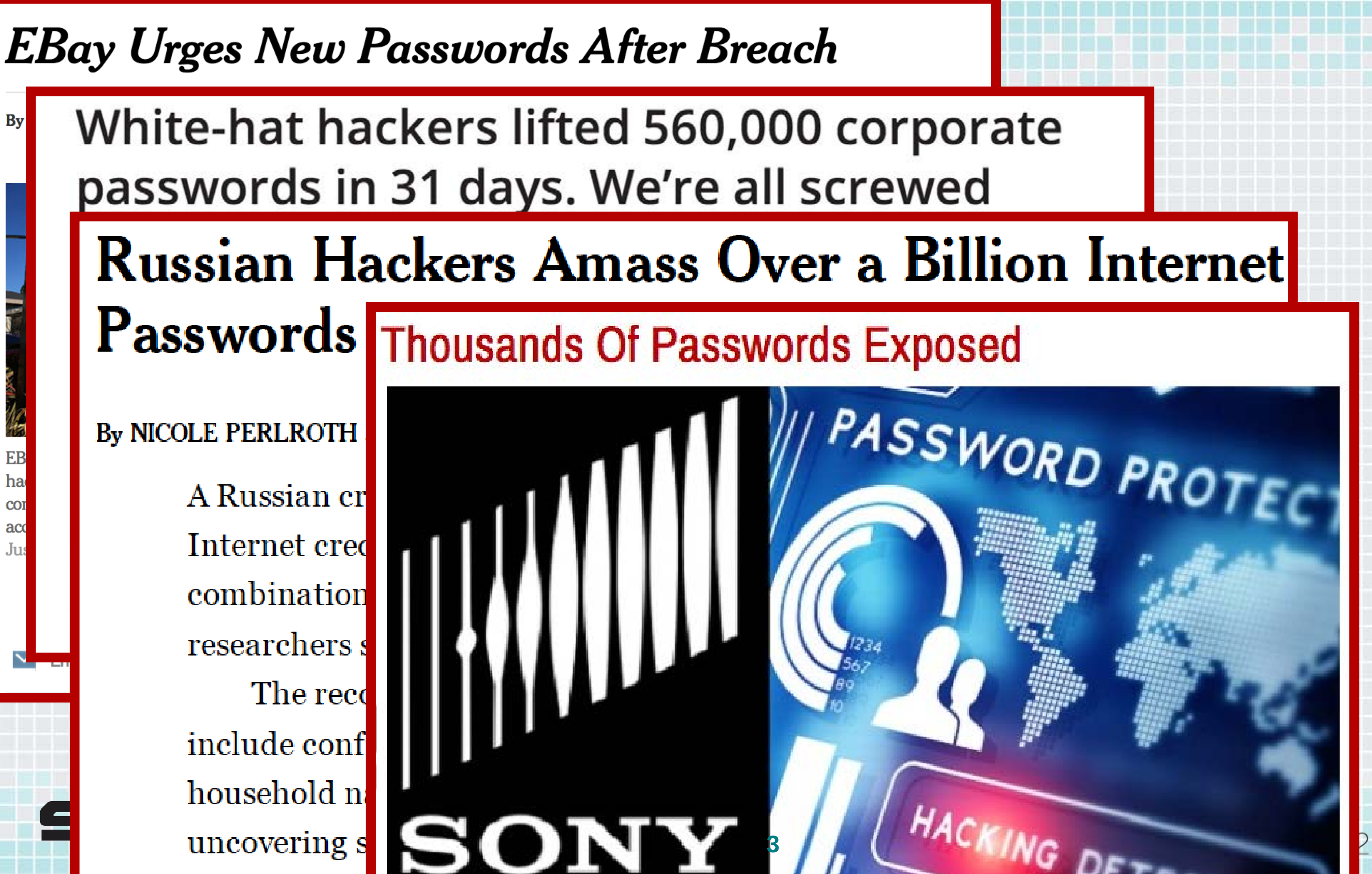
Zhiwei Li

* collaborated with Warren He, Devdatta Akhawe, and Dawn Song from UC Berkeley

Research Scientist
Shape Security
@liwaius

20 years later …

"On the Internet, nobody knows you're a dog."



EBay Urges New Passwords After Breach

By

EB
ha
co
ac
Ju

White-hat hackers lifted 560,000 corporate passwords in 31 days. We're all screwed

Russian Hackers Amass Over a Billion Internet Passwords

By NICOLE PERLROTH

A Russian cr
Internet cred
combination
researchers s
The reco
include conf
household n
uncovering s

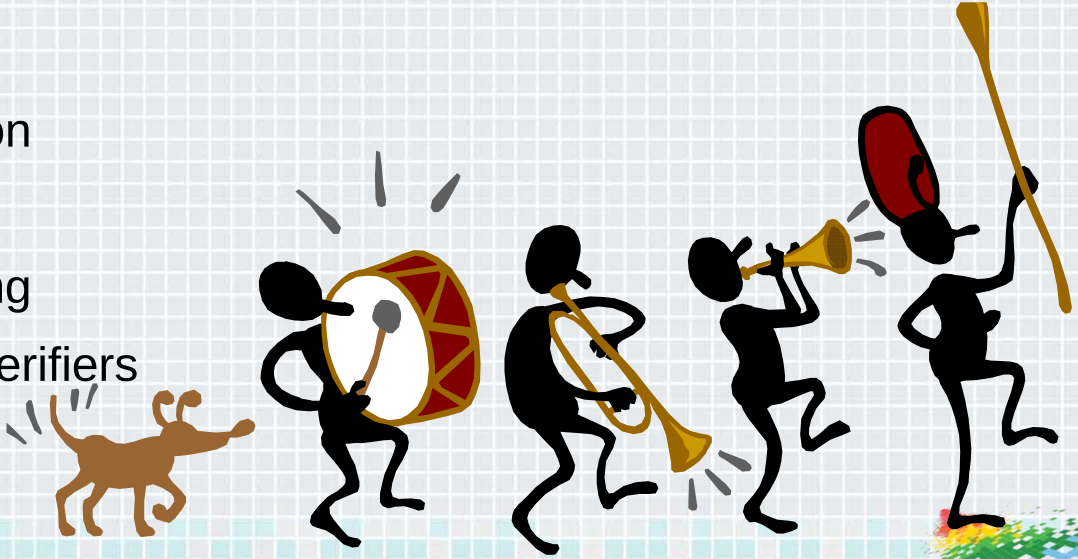
Thousands Of Passwords Exposed

Les coordonnées du superviseur
Sebastien
poste 48 08
5e étage
soc@tv5monde.org
Instagram
URL accueil admin site TV
http://informations.tv5

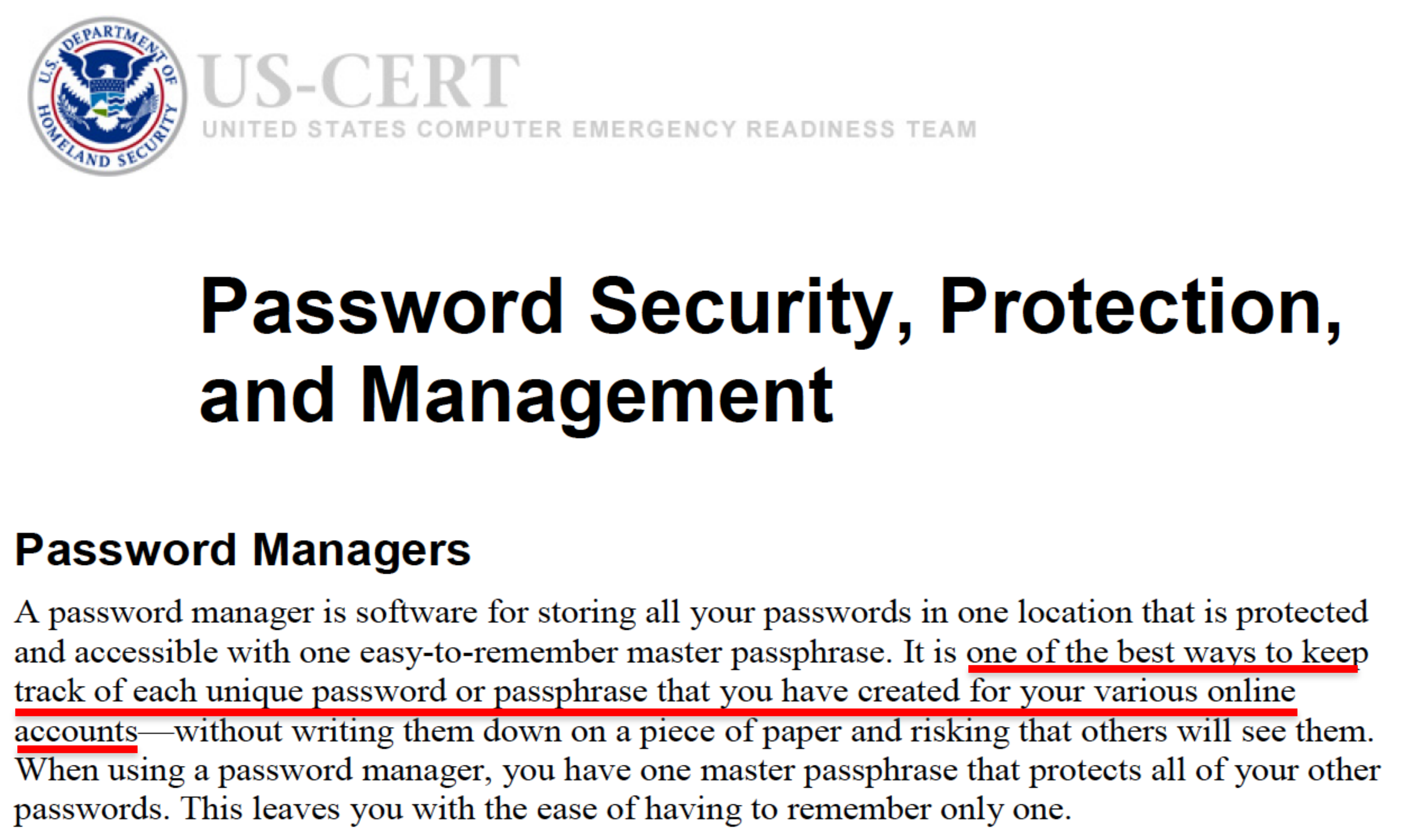
Kids Cyber Safe?

Password Managers to the rescue

- Physically Effortless
- Resilient to Phishing
- Memorywise Effortless
- Scalable for Users
- Resilient to Physical Observation
- Resilient to Throttled Guessing
- Resilient to Unthrottled Guessing
- Resilient to Leaks from Other Verifiers
- …



The New York Times	Apps to Protect Your Array of Passwords
PC EDITORS' CHOICE PCMAG.COM	XXXX is a must-use freeware tool that supports multiple operating systems and browsers
7x7SF	XXXX Offers NSA-Level Protection for Your Passwords
c|net	Keep All of Your Logins Secure With XXXX
lifehacker	XXXX Never Forget a Password Again
Xconomy	XXXX: Unbreakable Passwords That You Don't Have to Remember
TECHVIBES	XXXX Surpasses Gmail for Top Productivity App
TRENDHUNTER FIND BETTER IDEAS, FASTER	XXXX Wins Best Mobile App at CES 2014



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Password Security, Protection, and Management

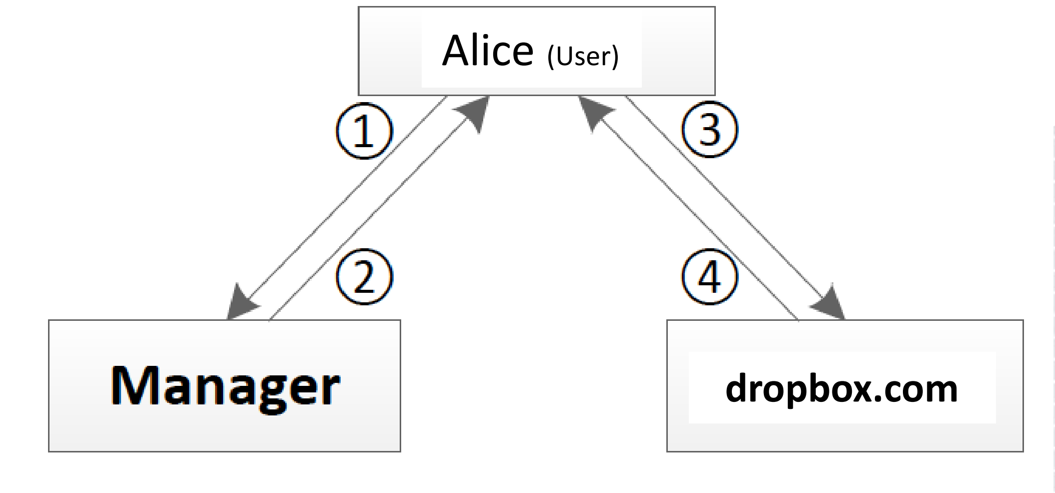
Password Managers

A password manager is software for storing all your passwords in one location that is protected and accessible with one easy-to-remember master passphrase. It is one of the best ways to keep track of each unique password or passphrase that you have created for your various online accounts—without writing them down on a piece of paper and risking that others will see them. When using a password manager, you have one master passphrase that protects all of your other passwords. This leaves you with the ease of having to remember only one.

Are they truly secure?

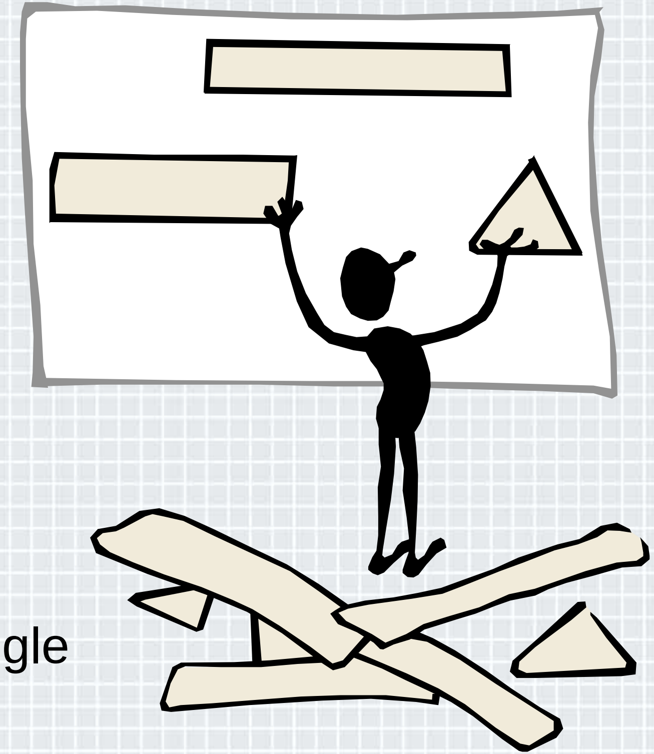
- LastPass
- RoboForm
- My1login
- PasswordBox
- NeedMyPassword

How does it work?



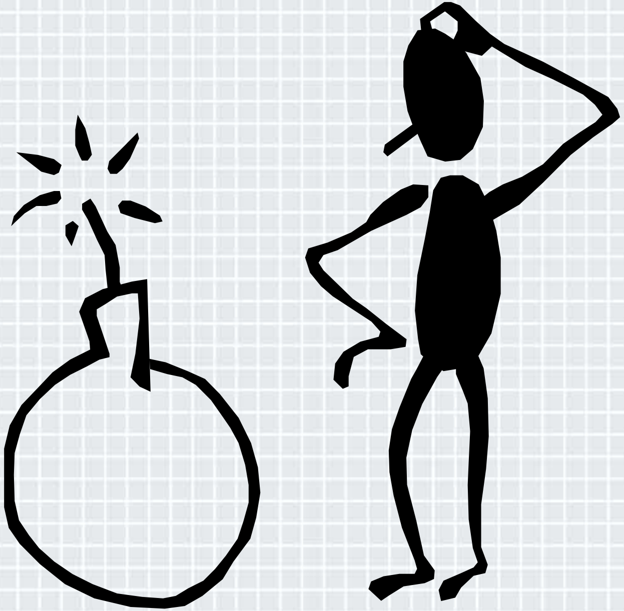
Security Goals

- Master Account Security
  - impossible for an attacker to authenticate as the user to the password manager
- Credential Database Security
  - ensure the CIA of the credential database
- Unlinkability
  - use of password manager should not allow colluding web applications to track a single user across websites



Threat model

- Web attacker
  - control web servers
  - DNS domains
  - get a victim to visit controlled domains

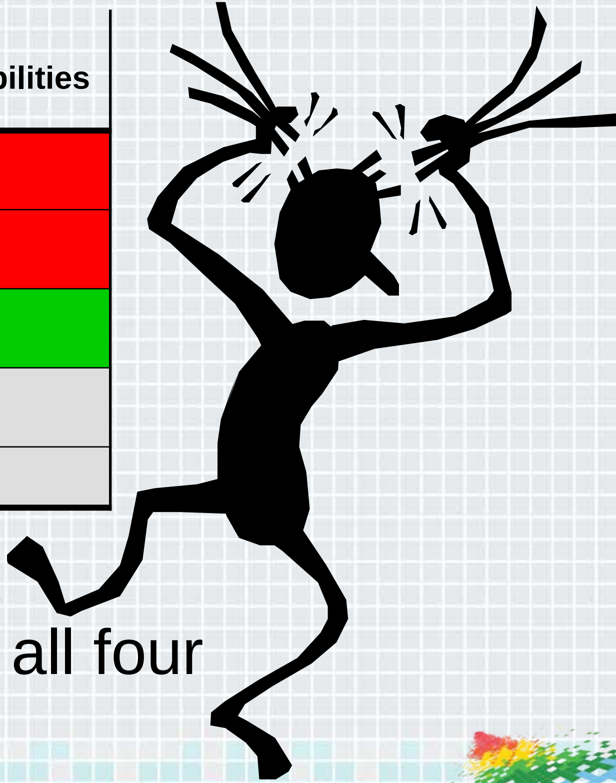


Four classes of vulnerabilities

	Bookmarklet Vulnerabilities	Web Vulnerabilities	Authorization Vulnerabilities	UI Vulnerabilities
LastPass	🟥	🟥	🟩	🟥
RoboForm	🟥	🟥	⬜	🟥
My1Login	🟥	🟩	🟥	🟩
PasswordBox	⬜	🟩	🟥	⬜
NeedMyPassword	⬜	🟥	🟩	⬜

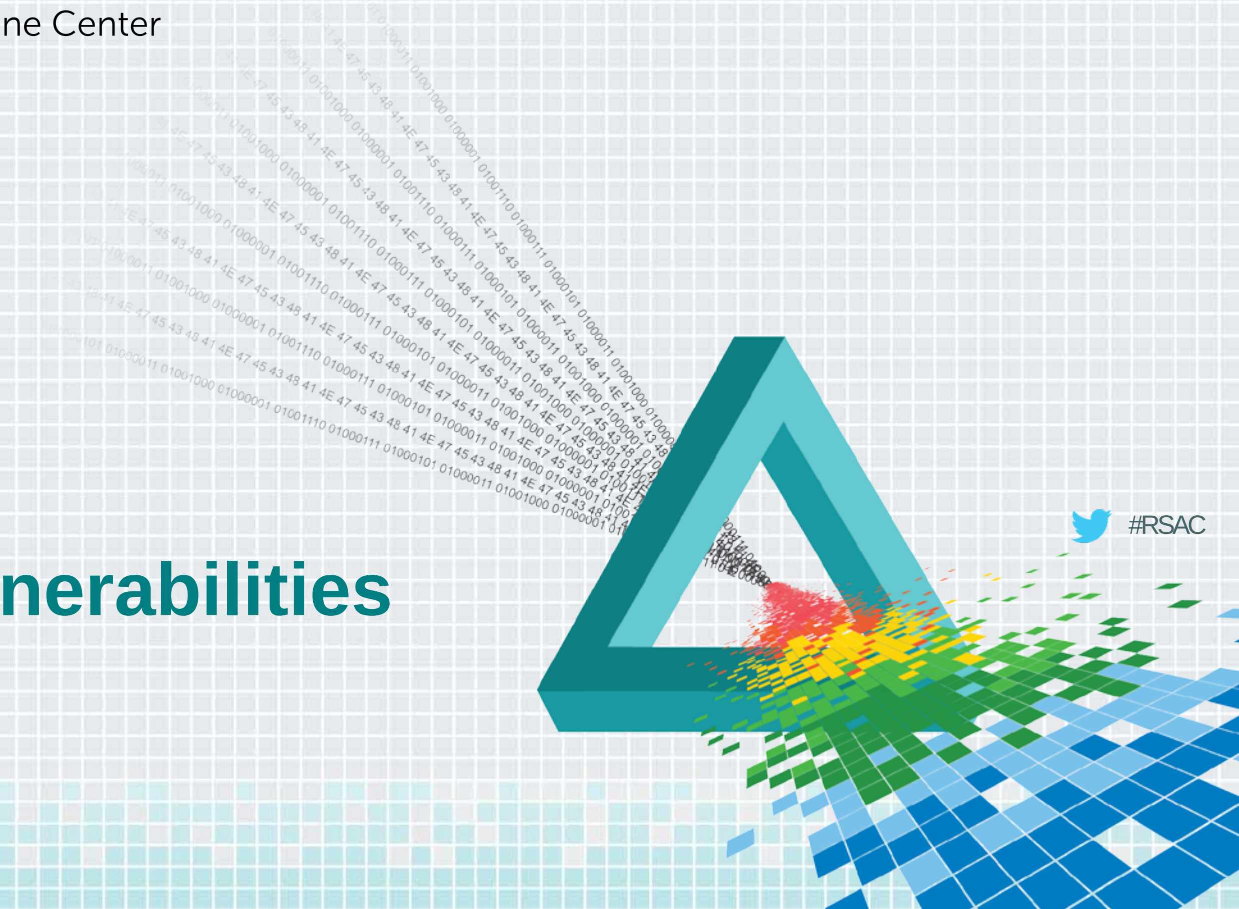
🟥	Vulnerable
🟩	Not discovered
⬜	NA

NO product was safe against all four



RSAConference2015

San Francisco | April 20-24 | Moscone Center

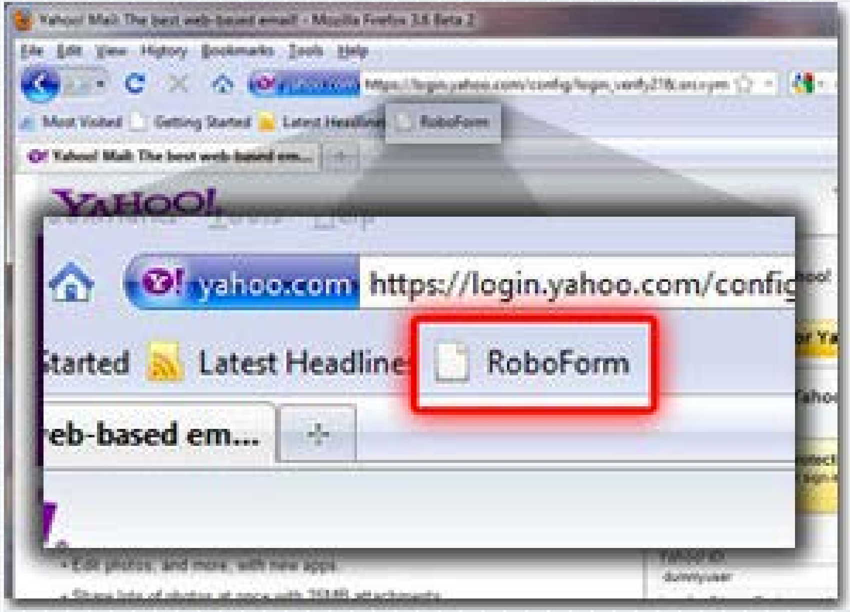


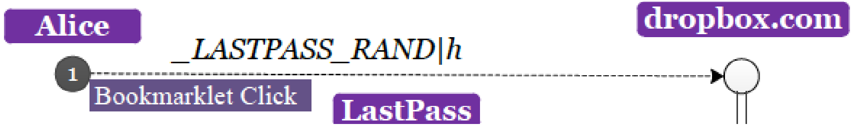
#RSAC

Bookmarklet Vulnerabilities

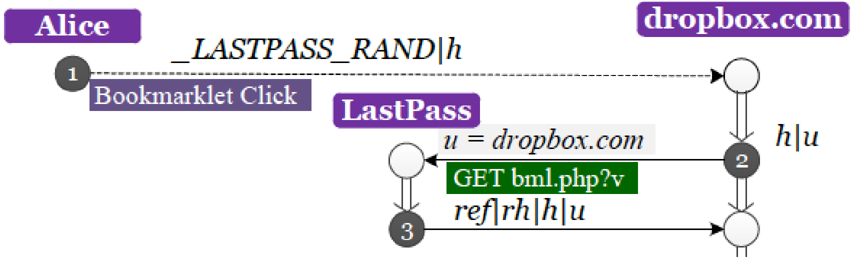
Bookmarklet

- A bookmarklet is a snippet of JavaScript code
  - install as a bookmark
  - when clicked, run in the context of the current page
  - interact with a login form

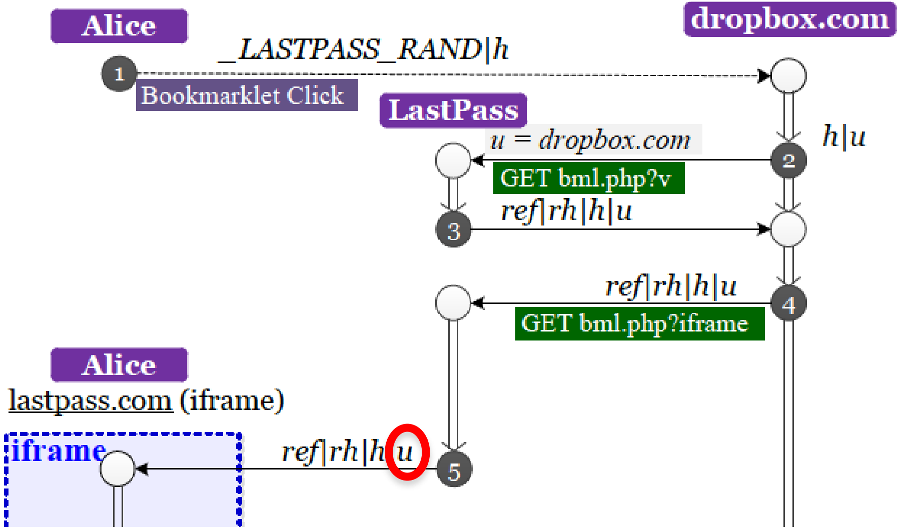

Yahoo! Mail: The best web-based email! - Mozilla Firefox 3.6 Beta 2
File Edit View History Bookmarks Tools Help
Most Visited
Getting Started
Latest Headlines
RoboForm
YAHOO!
yahoo.com
https://login.yahoo.com/config
tarted
Latest Headline
RoboForm
eb-based em...



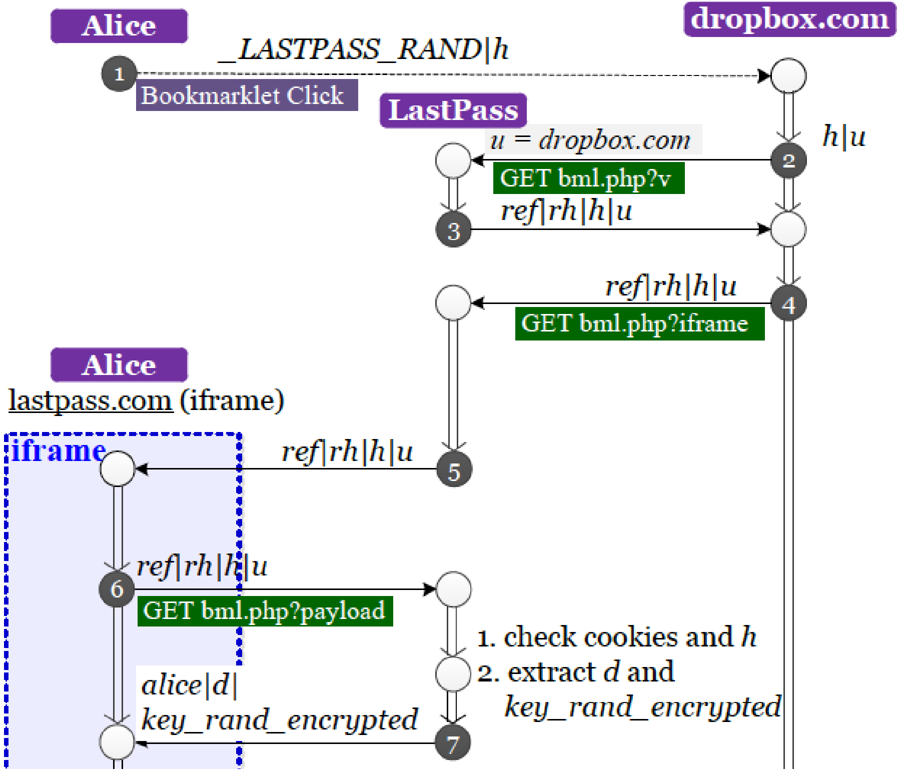
Alice clicks bookmarklet, which includes **_LASTPASS_RAND** and **h**



Bookmarklet code is a stub that loads the main code from lastpass.com

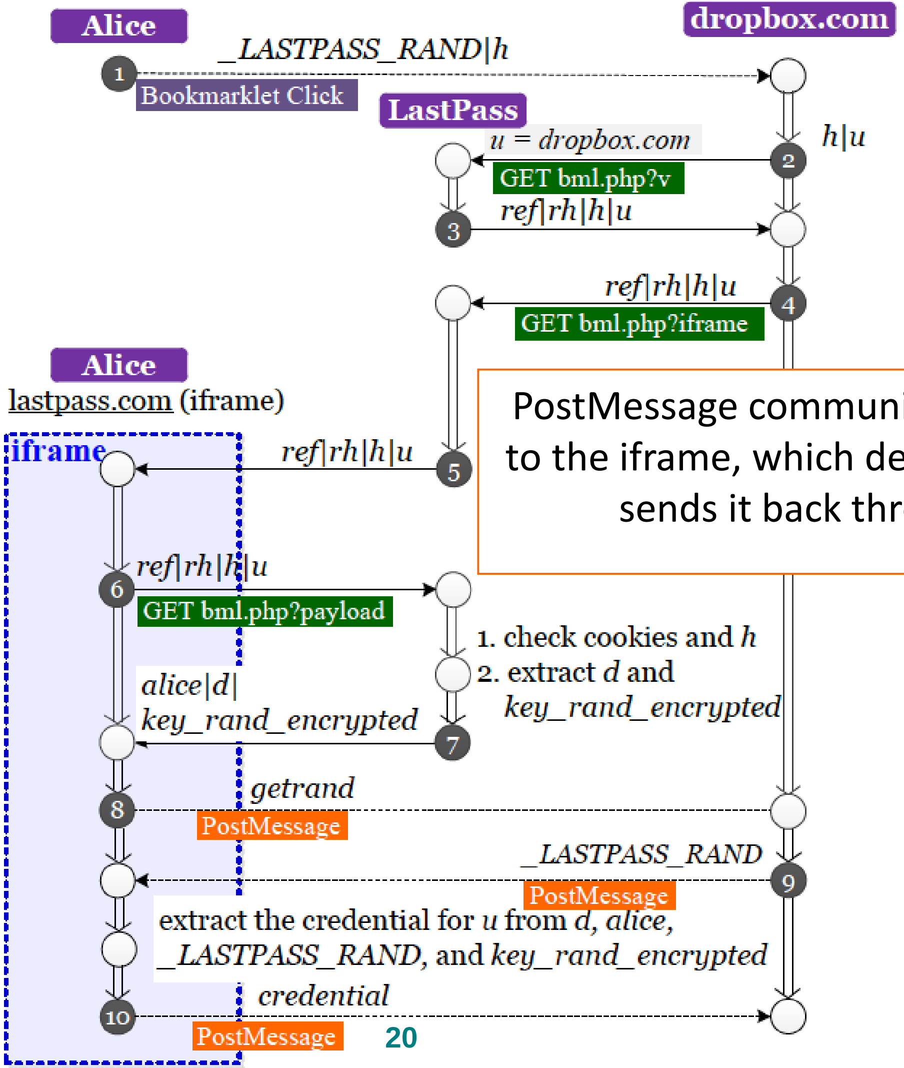


Bookmarklet loads a LastPass page in an iframe



The iframe loads Alice's encrypted master key and encrypted credential for dropbox.com (specified by a URL parameter).

This is done using a <script> tag in the iframe.



Alice

dropbox.com

_LASTPASS_RAND|h

1 Bookmarklet Click

LastPass

h|u

u = dropbox.com

2 GET bml.php?v

ref|rh|h|u

3

ref|rh|h|u

4 GET bml.php?iframe

Alice

lastpass.com (iframe)

iframe

ref|rh|h|u

5

ref|rh|h|u

6 GET bml.php?payload

1. check cookies and h
2. extract d and key_rand_encrypted

alice|d|
key_rand_encrypted

7

getrand

8 PostMessage

_LASTPASS_RAND

9 PostMessage

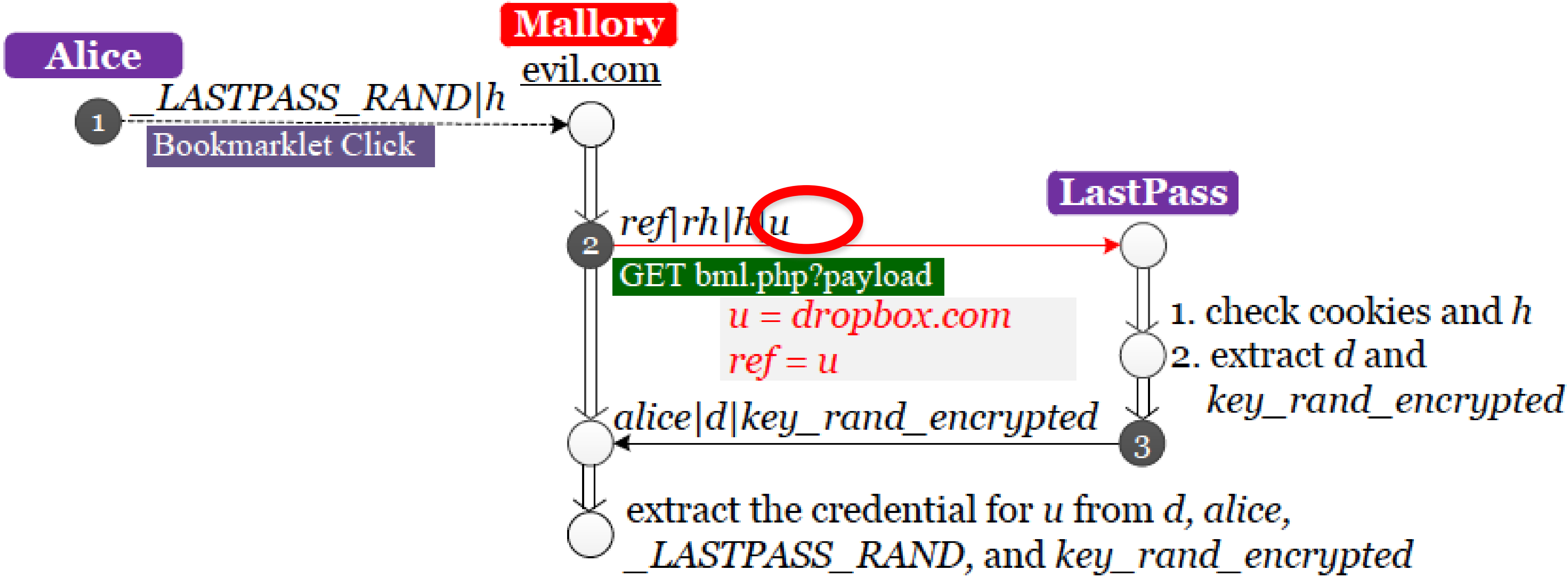
extract the credential for u from d, alice,
_LASTPASS_RAND, and key_rand_encrypted

credential

10 PostMessage

PostMessage communicates the decryption key to the iframe, which decrypts the credential and sends it back through PostMessage

LastPass Bookmarklet Attack



Alice
Mallory
evil.com
LastPass
1
_LASTPASS_RAND|h
Bookmarklet Click
2
ref|rh|h|u
GET bml.php?payload
u = dropbox.com
ref = u
1. check cookies and h
2. extract d and key_rand_encrypted
3
alice|d|key_rand_encrypted
extract the credential for u from d, alice, _LASTPASS_RAND, and key_rand_encrypted

Leaking sensitive data into untrusted pages

- All password managers that support bookmarklet leak their credentials
  - LastPass
  - RoboForm
  - My1login

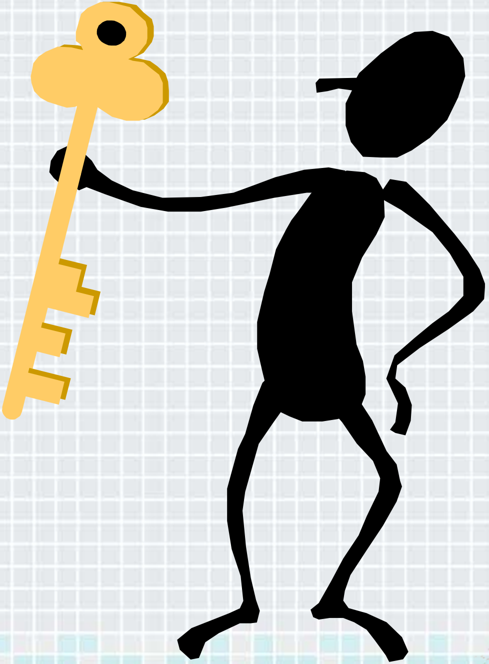
Classic Web Vulnerabilities

Web Vulnerabilities

- Subtleties of the web platform
- Focus on CSRF and XSS
- CSRF vulnerabilities
  - LastPass, RoboForm, and NeedMyPassword
- XSS vulnerability
  - NeedMyPassword

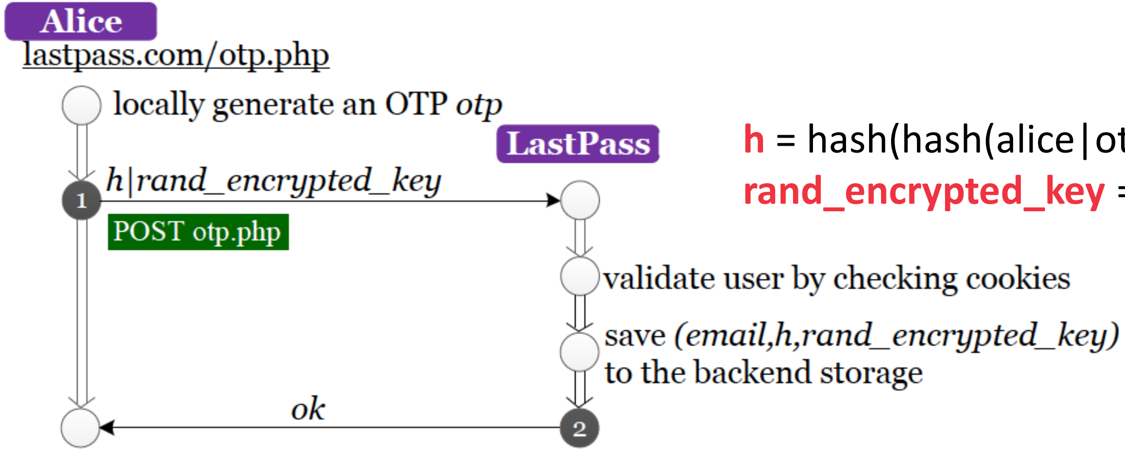
LastPass CSRF Vulnerability

- OTP feature
  - authentication code for the master account
  - only valid for one use
- Design flaw



h = hash(hash(alice|otp)|**otp**)

rand_encrypted_key = encrypt(**masterkey**, hash(alice|**otp**))



Alice

lastpass.com/otp.php

locally generate an OTP *otp*

LastPass

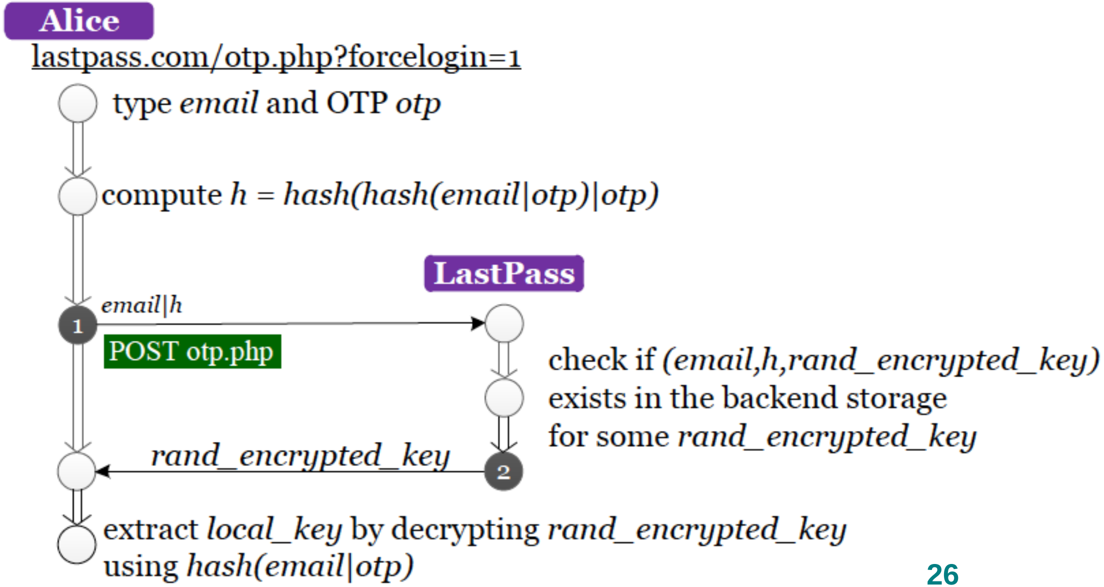
1 *h|rand_encrypted_key*

POST otp.php

validate user by checking cookies

save *(email,h,rand_encrypted_key)* to the backend storage

2 *ok*



Alice

lastpass.com/otp.php?forcelogin=1

type *email* and OTP *otp*

compute *h = hash(hash(email|otp)|otp)*

LastPass

1 *email|h*

POST otp.php

check if *(email,h,rand_encrypted_key)* exists in the backend storage for some *rand_encrypted_key*

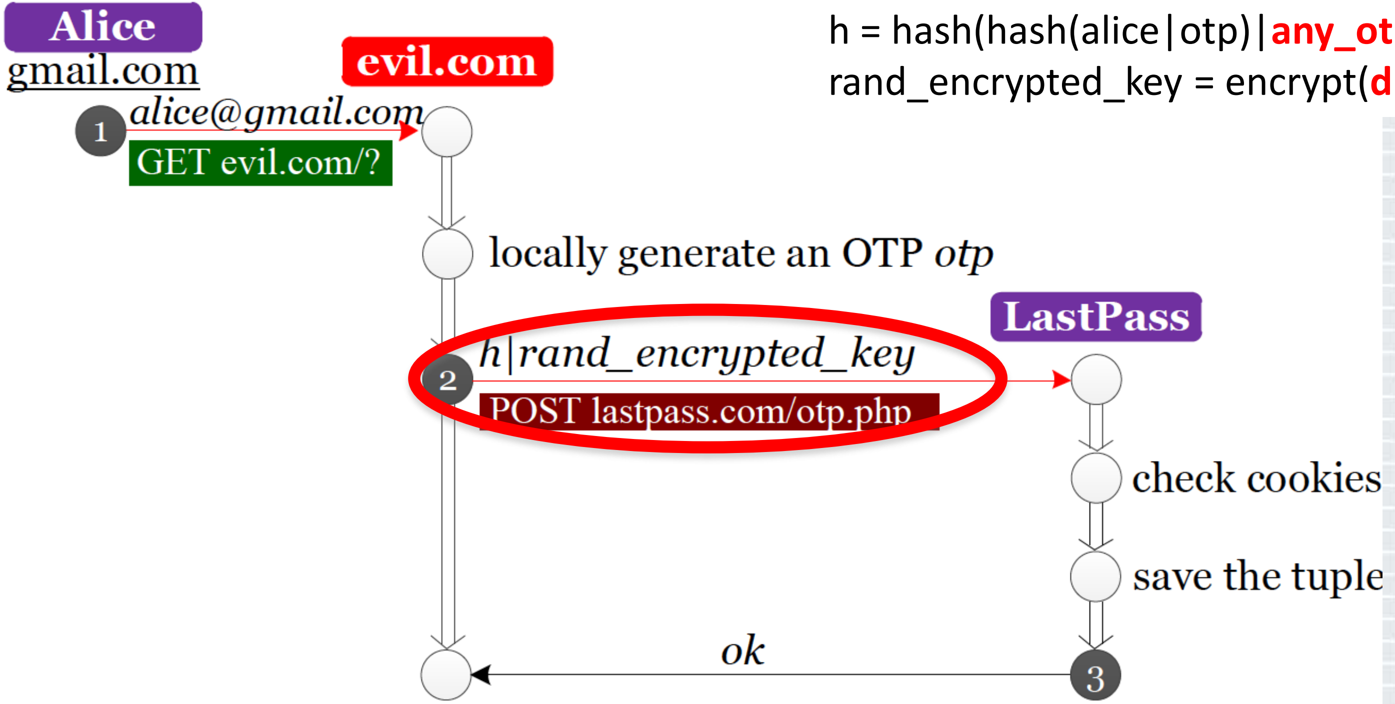
2 *rand_encrypted_key*

extract *local_key* by decrypting *rand_encrypted_key* using *hash(email|otp)*

OTP Attack

h = hash(hash(alice|otp)|**any_otp**)

rand_encrypted_key = encrypt(**dummy**, hash(alice|**any_otp**))



The attacker can then log into Alice's master account to view unencrypted information and delete credentials

RSA Conference2015

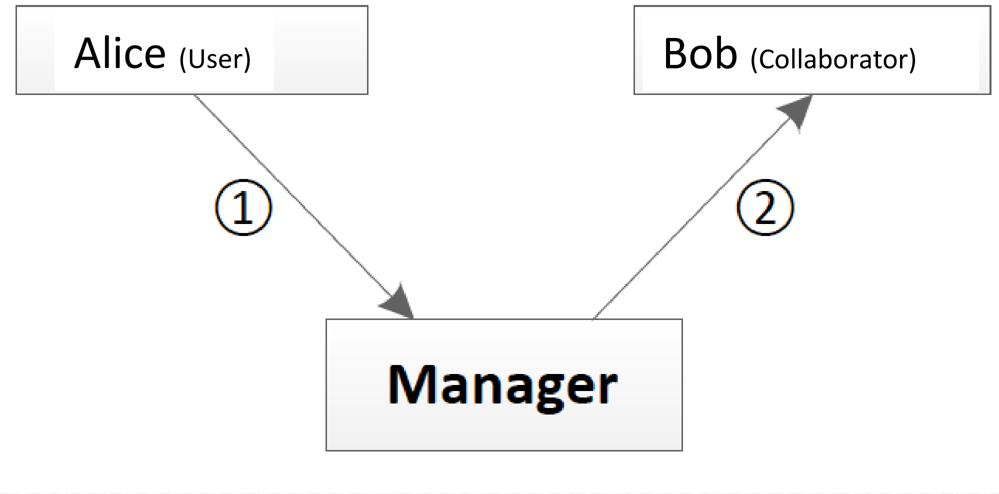
San Francisco | April 20-24 | Moscone Center

Authorization Vulnerabilities

#RSAC

Collaboration

- Ability to share passwords with a collaborator



Alice (User)

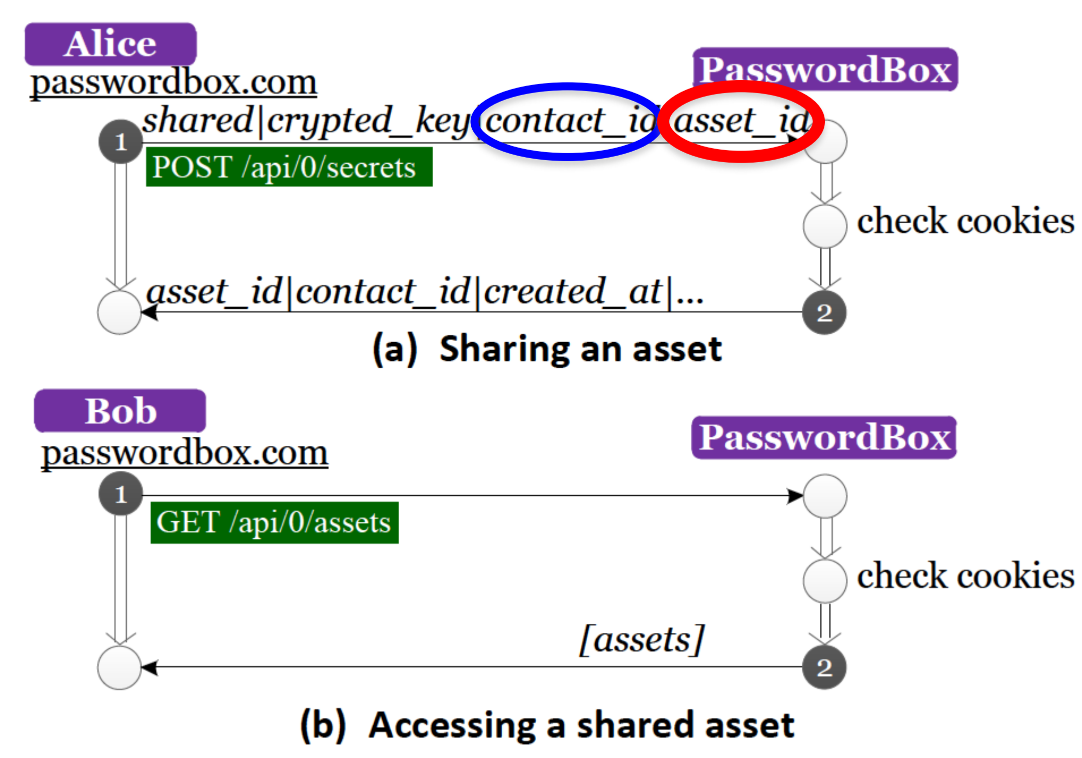
Bob (Collaborator)

Manager

- Alice requests to share a credential with Bob
- Password manager forwards the credential to Bob
- Both need accounts with the password manager

Authorization Vulnerabilities

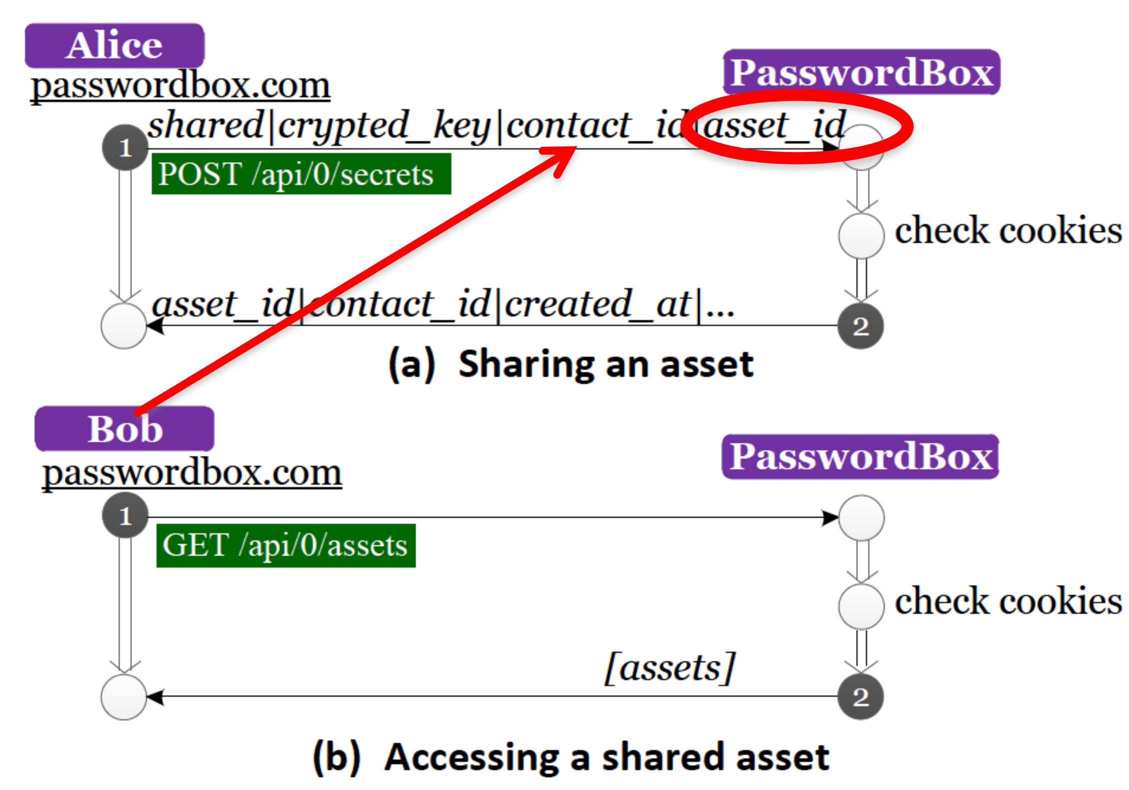
- 3 support credential sharing
- Both My1login and PasswordBox mistook authentication for authorization


Alice
passwordbox.com
PasswordBox
shared|crypted_key|contact_id|asset_id
1
POST /api/0/secrets
check cookies
asset_id|contact_id|created_at|...
2

(a) Sharing an asset

(b) Accessing a shared asset

PasswordBox


Alice
passwordbox.com
PasswordBox
shared|crypted_key|contact_id|asset_id
1
POST /api/0/secrets
check cookies
asset_id|contact_id|created_at|...
2

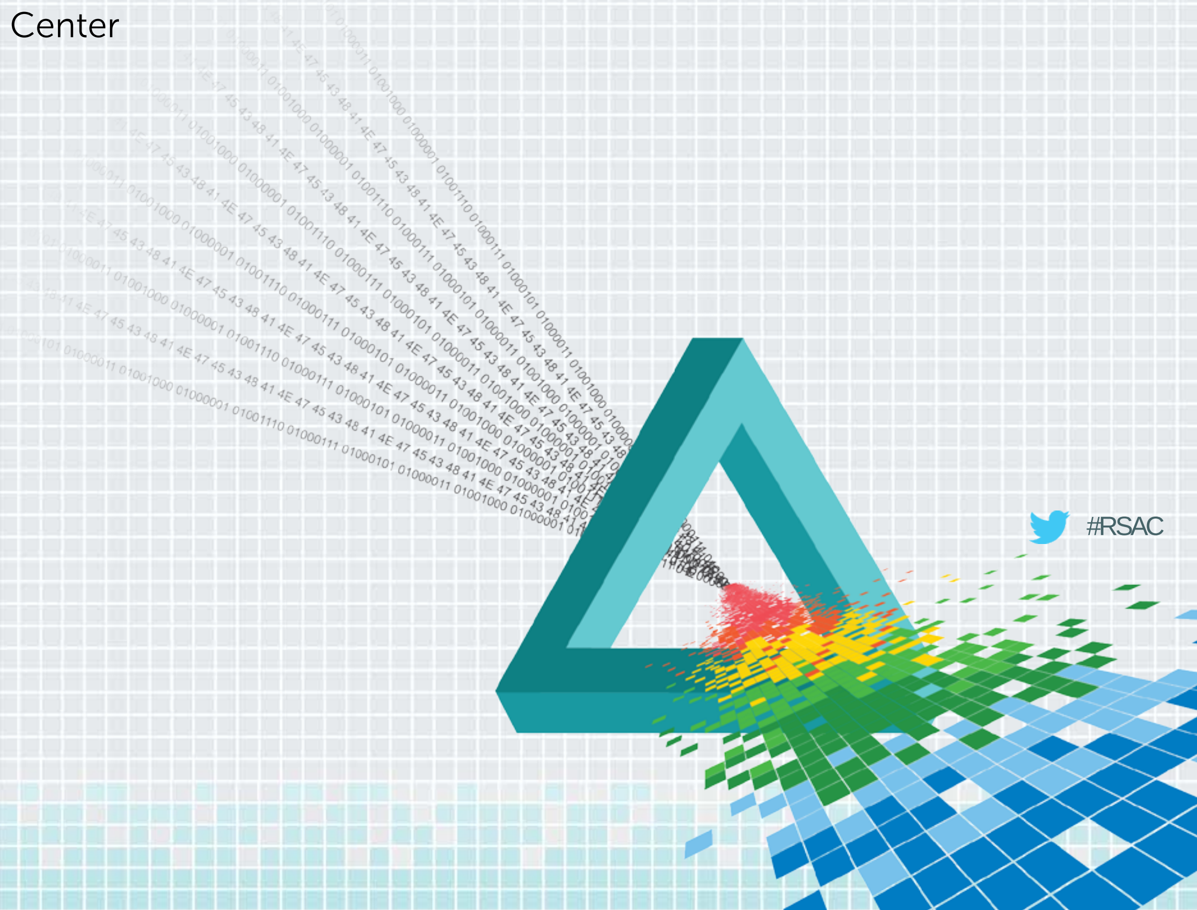
(a) Sharing an asset

(b) Accessing a shared asset

RSAConference2015

San Francisco | April 20-24 | Moscone Center

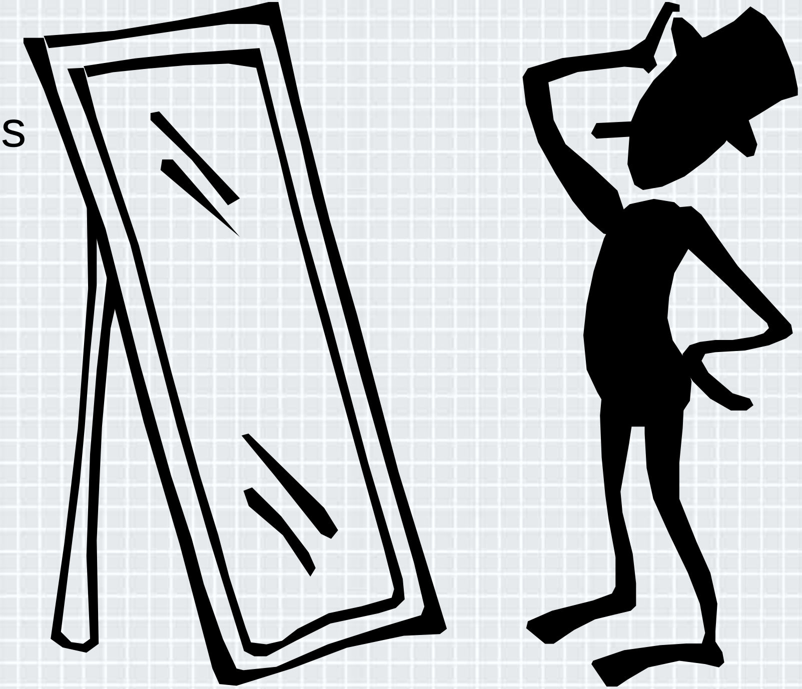
User Interface Vulnerabilities



#RSAC

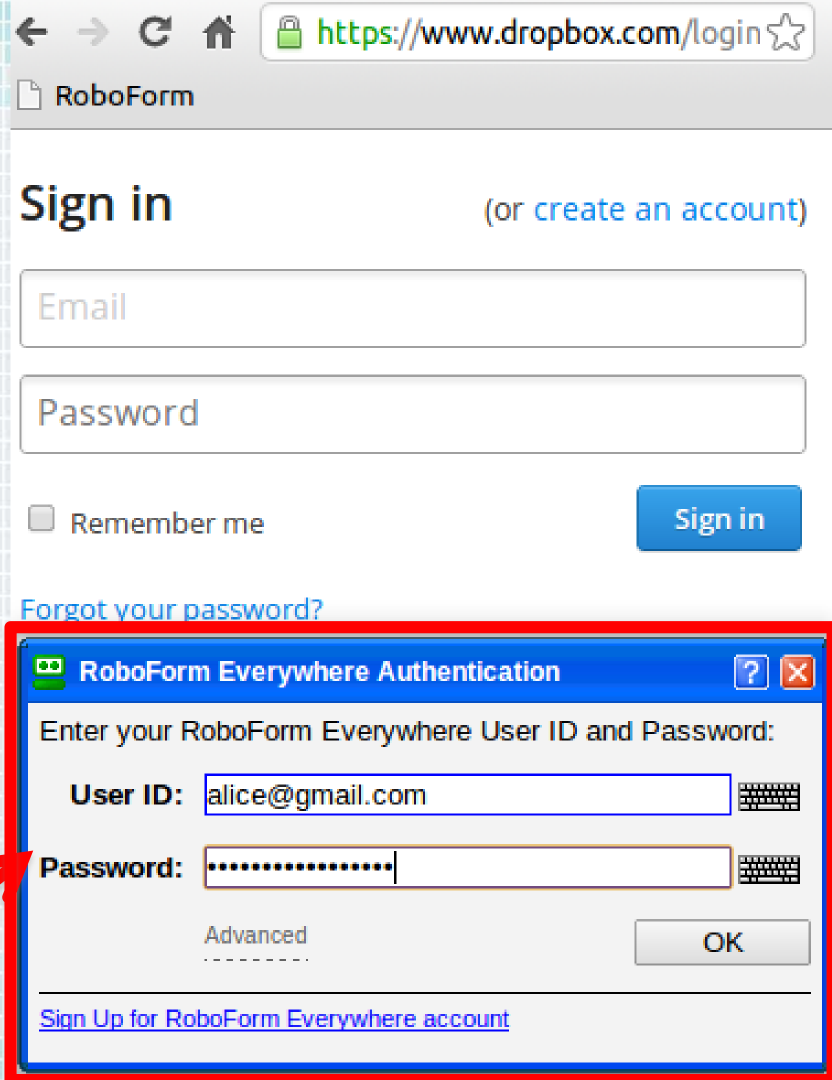
User Interface Vulnerabilities

- Resilient to Phishing
  - a major benefit of password managers
  - detects application
  - (auto-)fill the right password
- Vulnerable
  - LastPass
  - RoboForm



Logging into RoboForm

- Creates an iframe in the current web application to log in the user
- Attack
  - block the iframe
  - spoof an authentication dialog
  - steal master credentials



https://www.dropbox.com/login

RoboForm

Sign in (or create an account)

Email

Password

□ Remember me

Sign in

Forgot your password?

RoboForm Everywhere Authentication

Enter your RoboForm Everywhere User ID and Password:

User ID: alice@gmail.com

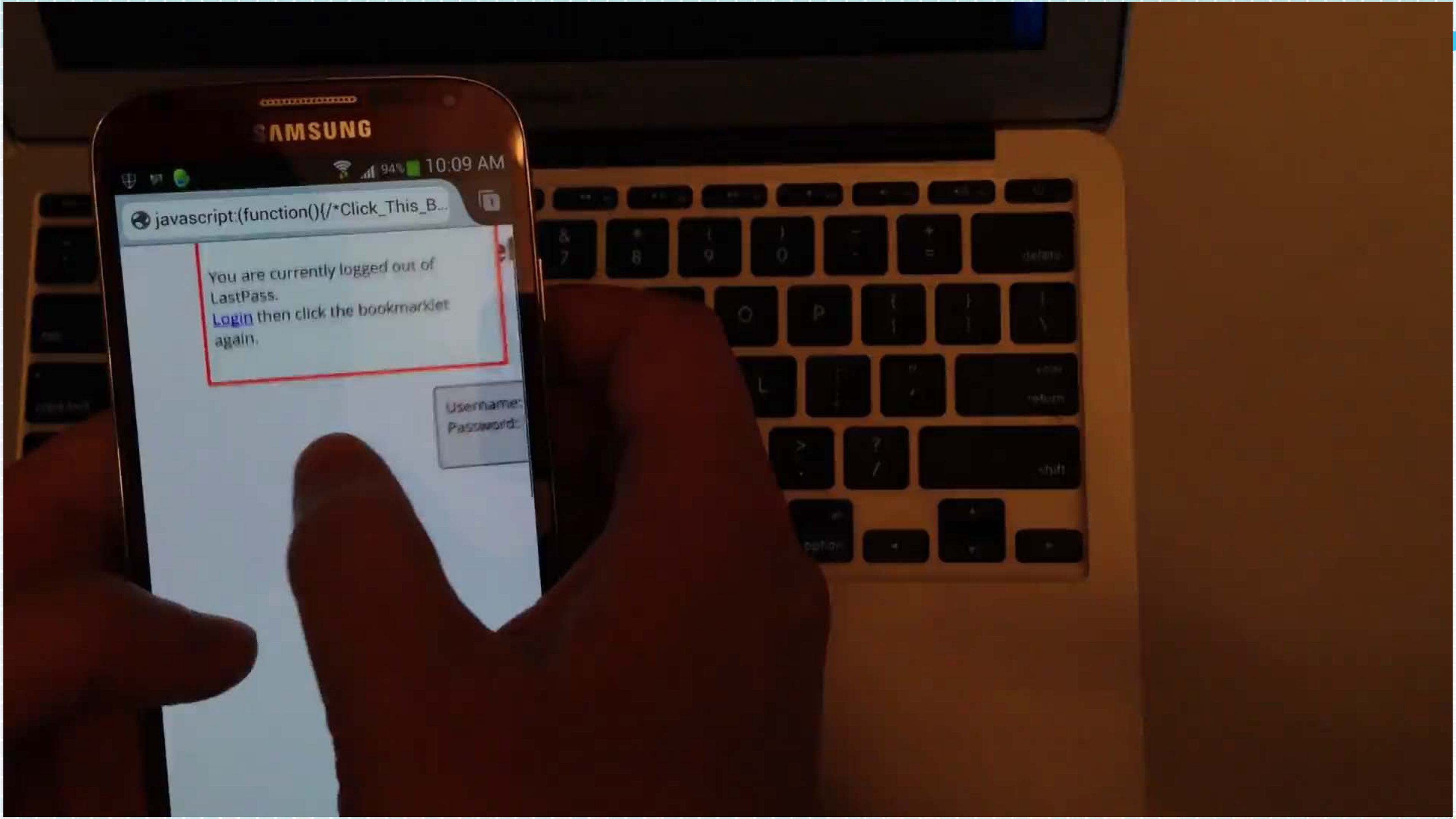
Password: ••••••••••••••••

Advanced

OK

Sign Up for RoboForm Everywhere account

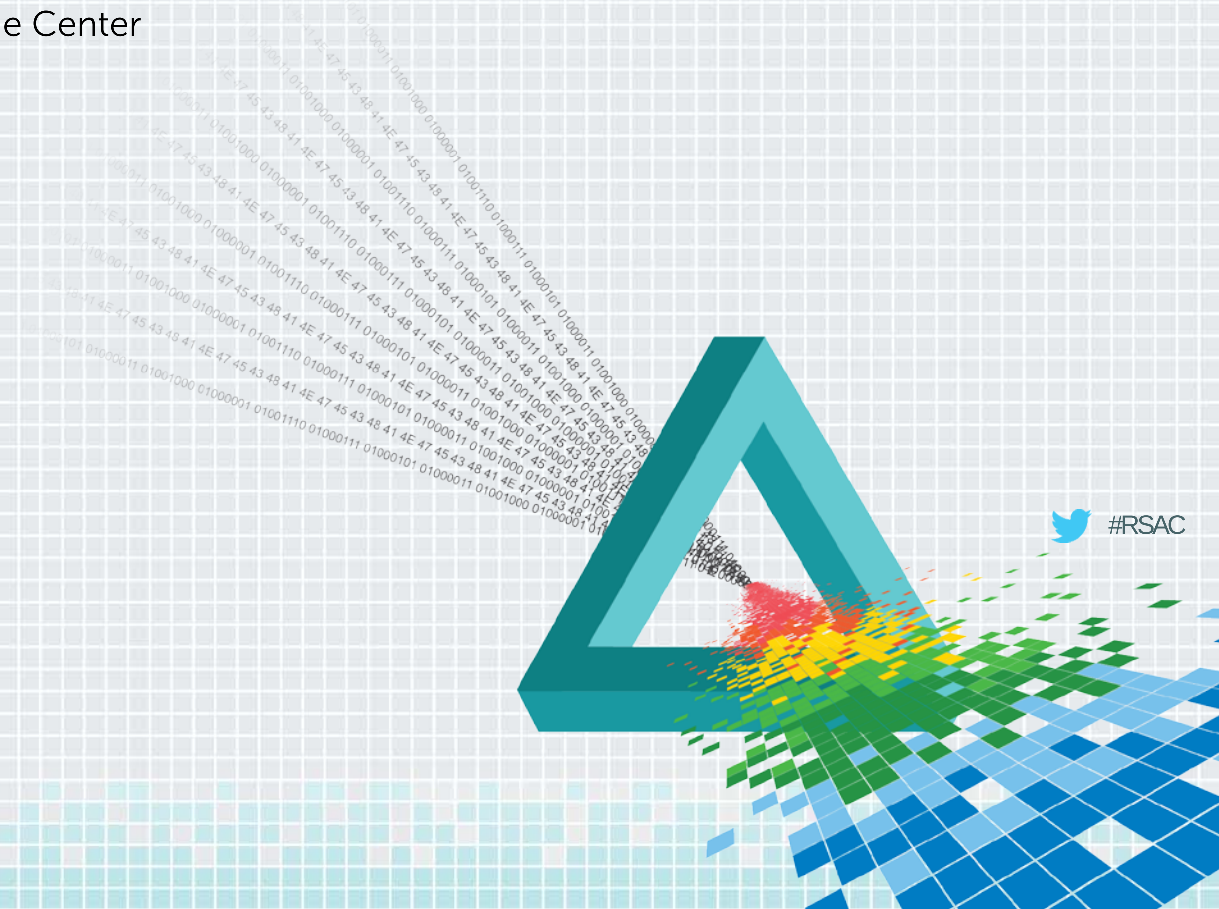
iframe



You are currently logged out of LastPass.
Login then click the bookmarklet again.

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

Mitigation

Apply Slide

- Bookmarklet Vulnerabilities
  - loads the password manager code in an iframe
  - `postMessage` with the right target
  - consider DJS (Defensive JavaScript) proposed by Karthikeyan Bhargavan
- Web Vulnerabilities
  - Content Security Policy (CSP)
  - CSRF prevention
- Authorization Vulnerabilities
  - simplify sharing logic
- UI Vulnerabilities
  - manually open a new tab

Take Homes

- Design and implement with security in mind
- Formalizing (better yet verifying) protocol pays off

Conclusions

- A wide spectrum of discovered vulnerabilities
  - logic mistakes
  - misunderstanding about the web security model
  - typical vulnerabilities like CSRF and XSS
- A single solution is unlikely
- Developing password manager entails a systematic, defense-in-depth approach

Stay Tuned.

http://pepperword.com